REMARKS

Claims 1-34 are pending in the present application.

In the office action mailed January 19, 2005 (the "Office Action"), claims 1-34 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,810,525 to Safadi et al. (the "Safadi patent").

The Safadi patent is directed to a system for verifying authorization during the purchase and receipt of services remotely at a subscriber terminal. Additionally, the system provides a mechanism that guards against workarounds where a purchase is not registered, but is provided to the subscriber terminal anyway, that is, obtain the service for free. Moreover, the system described in Safadi provides non-repudiation of a purchase transaction since a Network Operator is provided with absolute visibility and control of the purchasable services.

Operation of the system in the Safadi patent is described as follows. A request is made by a subscriber to purchase a service, for example, an impulse pay-per-use (IPPU) service. Generally, the request, or the IPPU selection, is sent from the subscriber to an access controller 14. The access controller 14 generates an encrypted message that includes, among other things, authorization settings for the IPPU selection and the cost for the IPPU selection. The encrypted message is then sent back to a subscriber terminal 16. In response, a secure processor 32 in the subscriber terminal 16 decrypts the message from the access controller 14 and determines whether the subscriber has sufficient credit entitlement to purchase the IPPU selection. If so, a secure "entitlement token" is generated by the secure processor 32 and provided to a client application resident in the subscriber terminal 16. In an alternative embodiment, the entitlement token is generated by the access controller 14 and provided to the subscriber terminal 16 rather than being generated by the subscriber terminal 16. Regardless of where the secure entitlement token is generated, the client application forwards the entitlement token to a server 18 having the IPPU selection. The server 18 decrypts the entitlement token and further checks the status of the subscriber's entitlement to receive the IPPU selection. If verified, the server forwards the IPPU selection content to the subscriber terminal 16. Encrypted selection content can be provided, in an alternative embodiment, and can be decrypted by the subscriber terminal 16. By having the server 18 check for entitlement, in addition to the subscriber terminal 16, the server 18 can further validate the legitimacy of the subscriber's entitlement to the requested service.

In an alternative embodiment described in the Safadi patent, the IPPU selection is first sent to a customer response center (CRC) before being forwarded to the access controller 14. This allows for the CRC to bill the subscriber for the requested service. Additionally, another billing system 20 can be informed of the IPPU transaction by the server 18 when it receives the entitlement token from the client application.

As previously mentioned, claims 1-34 were rejected under 35 U.S.C. 102(e) as being anticipated by the Safadi patent. As the Examiner is well aware, in order to support an anticipation rejection, a reference must disclose every limitation of the combination of limitations recited in the claim, and moreover, disclose the particular combination recited in the claim. Unless the Safadi patent describes all of the limitations recited by a claim, the Safadi patent cannot be relied upon as the basis for a rejection under 35 U.S.C. 102(e).

Claim 1 is patentably distinct from the Safadi patent because the Safadi patent fails to describe the combination of limitations recited by claim 1. For example, the Safadi patent fails to describe initiating a request to open a computer resource stored on the computer system. As previously discussed, the Safadi patent is directed to purchasing a service which is eventually provided to a subscriber terminal 16 (i.e., the computer system) by a server 18. The computer resource is not present in the subscriber terminal until after verification is completed and it is provided by the server. As such, initiating a request to open a computer resource stored on a computer system is not disclosed. The Examiner cites col. 2, lines 47-55 as disclosing the particular limitations. The material cited describes an embodiment where the secure entitlement token is a signed and encrypted entitlement token which is securely sent from the client application to the server 18 for decryption and authentication. This, however, does not describe initiating a request to open a computer resource stored on the computer system.

Additionally, another example of the deficiency of the Safadi patent is with respect to, under control of the remote application manager component, decrypting the token and authenticating a user of the computer system using authentication information stored on the token. As described in the Safadi patent, the secure entitlement token, if encrypted, is decrypted by the server 18. However, the remote application manager component is recited in claim 1 as being on the computer system. Even if the server 18 is considered to be analogous to the computer system, the Safadi patent fails to disclose opening the requested computer resource,

which is recited in claim 1 to be "stored on the computer system," when the user is authenticated, authorized, and has sufficient credit. In contrast to claim 1, upon verification of entitlement, the IPPU selection is simply forwarded to the subscriber terminal 16 by the server 18. Moreover, assuming that the server 18 is considered to be analogous to the computer system recited in claim 1, the Safadi patent does not describe the server 18 monitoring the usage of the opened computer resource to determine whether the user has sufficient credit to continue using the computer resource. The Safadi patent further fails to describe providing a notification when the monitored usage of the opened computer resource has exceeded the credit.

For the foregoing reasons, claim 1 is patentably distinct from the Safadi patent. Claims 2-10, which depend from claim 1, are similarly patentably distinct from the Safadi patent for at least the reason they are dependent from allowable claim 1. That is, each of the dependent claims further narrows the scope of the claim from which it depends, and consequently, if a claim is dependent from an allowable base claim, the dependent claim is also allowable.

Additionally, several of the dependent claims specifically recite limitations that are not disclosed in the Safadi patent. The Safadi patent is deficient in several respects. For example, the Safadi patent fails to describe an embodiment where the secure entitlement token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token, as recited in claim 3. Nor does the Safadi patent describe monitoring the usage of the opened computer resource by monitoring how long the user has been using the computer resource, as recited in claim 9. The Safadi patent further fails to describe providing a notification when the monitored usage of the opened computer resource has exceeded the credit by displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted, as recited in claim 10.

Although the Examiner has cited to material in the Safadi patent as disclosing the respective limitations of claims 3, 9, and 10, the cited material is deficient. For claim 3, the Examiner cited to material at col. 2, lines 7-10. The cited material states, "[i]f such verification is successful, the subscriber terminal generates a secure entitlement token for use by a client application residing in the subscriber terminal. The entitlement token may alternatively be generated by the access controller and forwarded to the subscriber terminal." There is no mention of a smart card, or storing the secure entitlement token on a smart card in the cited

material. If the Examiner maintains the assertion that the cited material discloses a token stored on a smart card that the remote application module component accesses to retrieve and decrypt the token, Applicants request the Examiner clarify the argument. With respect to claim 9, the Examiner cited to material at col. 6, lines 60-65. The cited material states, "[i]n this way, the server 18 can further validate the legitimacy of the subscriber's entitlement to the requested service. It also provides non-repudiation of the purchase transaction within the subscriber terminal, allowing the Network Operator to have absolute visibility and control of the purchasable services." The cited material, as understood by Applicants, does not disclose monitoring the usage of the opened computer resources by monitoring how long the user has been using the computer resource. It describes the benefits of having the server decrypt the entitlement token and independently verify entitlement of the service by the subscriber. If the Examiner maintains the assertion that the cited material discloses the limitation of claim 9, Applicants request the Examiner to clarify the argument. With respect to claim 10, the Examiner cited to col. 6, lines 60-65, and elaborated by indicating "absolute visibility." *See* the Office Action at page 6. As understood by the Applicants, "absolute visibility," as used in the context of the cited material, does not disclose displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted, as recited in claim 10. Absolute visibility suggests that the Network Operator has the ability to prevent provision of the requested service if entitlement is not verified at the server. As previously requested, if the Examiner maintains the assertion that the cited material discloses the limitations of claim 10, Applicants request the Examiner clarify the argument.

Consequently, in addition to the patentable distinction of claims 2-10 based on the dependency of these claims from allowable claim 1, several of the claims are also patentably distinct from the Safadi patent because the Safadi patent does not disclose the specific limitations recited by the respective dependent claim.

Therefore, the rejection of claims 1-10 under 35 U.S.C. 102(e) should be withdrawn.

Claims 11, 19, 27, and 31 are similarly patentably distinct from the Safadi patent. For example, with respect to claim 11, the Safadi patent fails to disclose, under the control of a client system, receiving from the server system a token including encrypted information

generated form the user information provided by the client system. As previously discussed, the server 18 in the Safadi patent *receives* the entitlement token. Additionally, the Safadi patent does not disclose receiving from the server system a remote application manager component, in addition to the token and at least one computer resource. As described in the Safadi patent, the server 18 simply provides the IPPU selection content to the subscriber terminal 16. There is no discussion of a remote application manager, or anything analogous, that is provided by the server 18 to the subscriber terminal 16. Moreover, the Safadi patent fails to disclose, under the control of the remote application manager component on the client system, monitoring the usage of the executing computer resource and providing a notification when the monitored usage has exceeded the user's credit. The Safadi patent appears to describe only a transaction where once entitlement is verified, that is, the subscriber has acceptable credit, the requested service is provided. Depletion of credit, or monitoring the depletion of credit while the service is used, is not disclosed in the Safadi patent.

With respect to claim 19, the Safadi patent fails to describe, under control of a server system, generating a token including encrypted information generated from the user information provided by the client system. The Safadi patent further fails to disclose sending the token to the client system. Additionally, the Safadi patent fails to disclose, under the control of the remote application manager component on the client system, decrypting the token and authenticating a user of the client computer system, and monitoring the usage of the executing computer resource and providing notification when the monitored usage has exceeded the user's credit. As previously discussed, the system described in the Safadi patent does not generate the entitlement token, and the subscriber terminal does not include a remote application manager component that decrypts the entitlement token or monitors usage of the executing computer resource.

Similarly with respect to claims 27 and 31, the Safadi patent fails to disclose the combination of limitations recited by the claims. For example, as previously discussed, the Safadi patent fails to disclose a client system, that is, a subscriber terminal 16, having a remote application manager that decrypts a token, monitors the usage of the opened computer resource, and provides notification when the monitored usage has exceeded the user's credit. The Safadi patent also fails to describe a server system having a token generation component and a client

interface component that transfers the token to a client computer along with a remote application manager component.

Claims 12-18, which depend from claim 11, claims 20-26, which depend from claim 19, claims 28-30, which depend from claim 27, and claims 32-34, which depend from claim 31, are also patentably distinct from the Safadi patent for at least the reason that these claims depend from a respective allowable base claim. As previously discussed with respect to dependent claims 2-10, several of dependent claims 12-18, 20-26, 28-30, and 32-34 are also patentably distinct because the Safadi patent fails to describe the particular limitation or limitations that are recited by the respective dependent claim.

For the foregoing reasons, claims 11-34 are patentably distinct from the Safadi patent, and the rejection of claims 11-34 under 35 U.S.C. 102(e) should be withdrawn.

All of the claims pending in the present application are in condition for allowance. Favorable consideration and a timely Notice of Allowance are earnestly solicited.

Respectfully submitted,

DORSEY & WHITNEY LLP

Kimton N. Eng
Registration No. 43,605
Telephone No. (206) 903-8718

KNE:ajs

Enclosures:
Postcard
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\documents\clients\micron technology\700\500767.01\500767.01 amendment.doc